Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Správa aktív, ochrana záznamov, súkromia a označovania informácií

Právny rámec, organizácia KB a strategické plánovanie (Blok I)

Kurz: Manažér kybernetickej bezpečnosti

prof. Ing. Tomáš Loveček, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Tomas.Lovecek@uniza.sk

Blok I.: Právny rámec, organizácia KB a strategické plánovanie

Hod. Obl.	Oblasti	Garant	Vyuč. hod.
2	Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti	Loveček	1,2
2	Správa aktív, ochrana záznamov, súkromia a označovanie informácií	Loveček	3,4
6	Riadenie kybernetických hrozieb a rizík	Loveček	5,6,7,8,9,10

Hodina	Začiatok	Koniec	Rozsah
1	8:00	8:45	0:45
2	8:45	9:30	0:45
3	9:45	10:30	0:45
4	10:30	11:15	0:45
5	11:30	12:15	0:45
6	13:00	13:45	0:45
7	13:45	14:30	0:45
8	14:45	15:30	0:45
9	15:30	16:15	0:45
10	16:30	17:15	0:45

Správa aktív, ochrana záznamov, súkromia a označovanie informácií

- Informačné aktíva, informačné systémy a siete, inventarizácia, klasifikácia a označovanie informácií
- Atribúty informácií (integrita, dôvernosť, dostupnosť, autenticita, nepopierateľnosť) a spôsob ich ochrany (organizačné, personálne, fyzické a technologické opatrenia)
- Manažment aktív (ISO 55000)
- Všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Normatívne požiadavky Zákona o KB

- Prevádzkovateľ základnej služby je ďalej povinný **analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb** s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu. *(§19 ods.6), písm. f)*

- Bezpečnostné opatrenia sa prijímajú aspoň pre **správu aktív** a riadenie kybernetických hrozieb a rizík. *(§20 ods.2), písm. c)*

Normatívne požiadavky Vyhlášky NBÚ č.227/2025 Z.z.

- Aktívum sa identifikuje a vedie v evidencii aktív. Evidencia aktív sa skladá z identifikovateľných primárnych aktív a podporných aktív.
- Aktíva sa identifikujú tak, že sú jednoznačne určené hranice jednotlivých sietí a informačných systémov a rozhrania medzi určenými hranicami.
- Evidencia aktív je centralizovane riadená a zodpovedá aktuálnemu stavu.
- Evidencia aktív sa môže skladať z textovej časti, tabuľkovej časti alebo grafickej časti a jej súčasťou je aj označenie bezpečnostných funkcií podporných aktív alebo odkazy na príslušnú časť bezpečnostnej dokumentácie týchto funkcií.
- Evidencia aktív obsahuje najmä identifikáciu a evidenciu
  a) primárnych aktív,
  b) podporných aktív,
  c) vlastníkov aktív,
  d) zodpovedných osôb za identifikáciu a evidenciu aktív.

- Podporné aktívum, ktoré súvisí s viacerými primárnymi aktívami, preberá najvyššiu hodnotu zo súvisiacich aktív.

Normatívne požiadavky zákona o ITVS

- Správca – orgán riadenia (UNIZA) je na úseku obstarávania a implementácie informačných technológií verejnej správy povinný **zabezpečiť riadenie aktív**. *(§15 ods. 1), písm. u))*
- V rámci zabezpečenia riadenia aktív v informačných technológiách verejnej správy správca *(§15 ods. 8))*:

  a) identifikuje a udržiava zoznam svojich aktív,

  b) vyhodnocuje možnosti využitia existujúcich informačných technológií alebo informačných technológií určených na spoločné využitie viacerými orgánmi riadenia a možnosti zdieľania svojich aktív s iným orgánom riadenia (napr. ministerstvo, obec, vyšší územný celok, právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti, atď.),

  c) identifikuje časti aktív, ktorých nedostupnosť alebo znížená kvalita má zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb,

  d) plánuje životný cyklus aktív v súlade so strategickými plánmi rozvoja informačných technológií verejnej správy a s aktuálnymi potrebami ich prevádzky.

Normatívne požiadavky zákona o ITVS

- V rámci zabezpečenia riadenia konfigurácií je správca povinný udržiavať zoznam konfigurácií svojich aktív. *(§15 ods. 9), písm. b))*
- V rámci nastavenia riadenia prevádzky informačných technológií verejnej správy **je správca povinný klasifikovať aktíva** (podľa nedostupnosti alebo zníženej kvality majúc zásadný vplyv na poskytovanie služieb), a to najmä s použitím kritérií potrieb konkrétnych služieb verejnej správy a dodržania povinností (dodržiavať princíp transparentnosti, princíp proporcionality a princíp hospodárnosti a efektívnosti). *(§16 ods. 2), písm. b))*

Normatívne požiadavky zákona o ITVS

- **Kategória II**
- **Identifikácia všetkých významných informačných aktív** v organizácii správcu a **určenie ich vlastníka**, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.
- **Zaradenie informačných aktív** podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu **do určených klasifikačných stupňov**, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu.
- Klasifikačné stupne pre informačné aktíva ustanovuje osobitný predpis (Vyhláška NBÚ, ktorou sa ustanovuje obsah bezpečnostných opatrení).

- **Kategória III**
- **Vytvorenie a udržiavanie zoznamu informačných aktív každého organizačného útvaru** organizácie správcu, ktorý je zároveň ich vlastníkom a ktorý určí požiadavky na dôvernosť, dostupnosť a integritu každého informačného aktíva v jeho vlastníctve.

Normatívne požiadavky STN ISO/IEC 27001:2023 (Príloha A.1)

- Musí sa vypracovať a udržiavať inventárny zoznam informácií. (5.9)
- Informácie sa musia klasifikovať podľa potrieb organizácie v oblasti informačnej bezpečnosti na základe požiadaviek na dôvernosť, integritu, dostupnosť a príslušných zainteresovaných strán. (5.12)
- Musí sa vypracovať a implementovať vhodný súbor postupov na označovanie informácií v súlade s klasifikačnou schémou prijatou organizáciou. (5.13)

Inventárny zoznam podľa STN ISO/IEC 27002:2023 (5.9)

- Organizácia by mala **identifikovať** svoje **informácie a iné súvisiace aktíva** a **určiť ich dôležitosť** z hľadiska informačnej bezpečnosti.
- Inventárny zoznam informácií a iných súvisiacich aktív by mal byť presný, aktuálny, konzistentný a zosúladený s ostatnými zoznamami.
- Možnosti zabezpečenia presnosti inventárneho zoznamu informácií a iných súvisiacich aktív zahŕňajú automatické vynútenie aktualizácie inventárneho zoznamu v procese inštalácie, zmeny alebo odstránenia aktíva.
- V prípade potreby by sa do inventárneho zoznamu malo zahrnúť aj umiestnenie aktíva.
- Inventárny zoznam nemusí byť len jeden zoznam informácií a iných súvisiacich aktív.
- Vzhľadom na to, že inventárny zoznam by mali udržiavať príslušné funkcie, možno ho chápať ako súbor dynamických inventárov, ako sú inventáre **informačných aktív, hardvéru, softvéru, virtuálnych strojov (VM), zariadení, personálu, kompetencií, schopností a záznamov.**
- **Každé aktívum by malo byť klasifikované v súlade s klasifikáciou informácií**, ktoré sú s týmto aktívom spojené.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Inventárny zoznam podľa STN ISO/IEC 27002:2023 (5.9)

- **Granularita inventárneho zoznamu** informácií a iných súvisiacich aktív **by mala byť na úrovni zodpovedajúcej potrebám organizácie**.
- Niekedy nie je možné zdokumentovať konkrétne prípady aktív v životnom cykle informácií vzhľadom na povahu aktíva. Príkladom krátkodobého aktíva je inštancia virtuálneho stoja, ktorého životný cyklus môže mať krátke trvanie.
- V prípade identifikovaných informácií a iných súvisiacich aktív by sa malo priradiť vlastníctvo aktív jednotlivcovi alebo skupine a mala by sa určiť klasifikácia.
- **Inventárne zoznamy** informácií a iných súvisiacich aktív **podporujú aj riadenie rizík**, audítorské činnosti, riadenie zraniteľností, reakciu na incidenty a riadenie obnovy.
- Ďalšie informácie o správe aktív informačných technológií (IT) nájdete v norme **ISO/IEC 19770-1 Specifies requirements for an IT asset management**. Ďalšie informácie o správe aktív nájdete v norme ISO 55001.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Klasifikácia informácií podľa STN ISO/IEC 27002:2023 (5.12)

- Organizácia by mala **vypracovať špecifickú politiku klasifikácie informácií** a oznámiť ju všetkým príslušným zainteresovaným stranám.
- Organizácia by mala v klasifikačnej schéme **zohľadniť požiadavky na dôvernosť, integritu a dostupnosť.**
- **Klasifikácie by mali zohľadňovať obchodné potreby** na zdieľanie alebo obmedzenie informácií, na ochranu integrity informácií a na zabezpečenie dostupnosti, **ako aj právne požiadavky.**
- Aktíva iné ako informácie sa môžu klasifikovať aj v súlade s klasifikáciou informácií, ktoré sú v aktívach uložené, nimi spracované alebo nimi aktíva narábajú či ich chránia.
- Vlastníci informácií by mali byť zodpovední za ich klasifikáciu.
- Klasifikačná schéma by mala zahŕňať kritériá na preskúmanie klasifikácie v priebehu času.

Klasifikácia informácií podľa STN ISO/IEC 27002:2023 (5.12)

- Príklad schémy klasifikácie dôvernosti informácií založenej na štyroch úrovniach:
  a) zverejnenie nespôsobuje žiadnu škodu;
  b) zverejnenie spôsobí menšie poškodenie dobrého mena alebo menší prevádzkový vplyv;
  c) zverejnenie má významný krátkodobý vplyv na prevádzku alebo obchodné ciele;
  d) zverejnenie má vážny vplyv na dlhodobé obchodné ciele alebo ohrozuje prežitie organizácie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Klasifikácia informácií podľa Vyhlášky NBÚ č. 227/2025 Z.z.

- Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako:
  a) Verejné informačné aktíva
  b) Interné informačné aktíva
  c) Chránené informačné aktíva
  d) Prísne chránené informačné aktíva
- Z hľadiska integrity sú klasifikačné stupne definované ako:
  a) Nízka
  b) Stredná
  c) Vysoká
- Z hľadiska dostupnosti sú klasifikačné stupne definované ako:
  a) Nízka
  b) Stredná
  c) Vysoká
- Bližší popis na:
  - https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2025/227/20250901#poznamky.poznamka-1

Označovanie informácií podľa STN ISO/IEC 27002:2023 (5.13)

- Mal by sa vypracovať a zaviesť vhodný súbor postupov na označovanie informácií v súlade so systémom klasifikácie informácií prijatým organizáciou.
- Postupy označovania informácií by sa mali vzťahovať na informácie a iné súvisiace aktíva vo všetkých formátoch.
- Označenia by mali byť ľahko rozpoznateľné.
- Postupy môžu definovať:

  a) prípady, keď sa vynecháva označovanie (napr. označovanie nedôverných informácií s cieľom znížiť pracovné zaťaženie),

  b) ako označovať informácie odoslané elektronickými alebo fyzickými prostriedkami či na nich uložené alebo informácie v akomkoľvek inom formáte,

  c) ako postupovať v prípadoch, keď označovanie nie je možné (napr. z dôvodu technických obmedzení).

Označovanie informácií podľa STN ISO/IEC 27002:2023 (5.13)

- Príklady techník označovania zahŕňajú:
  a) fyzické označenie;
  b) záhlavia a päty;
  c) metadáta;
  d) vodoznak;
  e) pečiatky.

f) Postupy by mali popisovať, ako pripojiť metadáta k informáciám, aké značky používať a ako by sa malo s údajmi zaobchádzať v súlade s informačným modelom organizácie a architektúrou IKT.

g) Personál a ostatné zainteresované strany by mali byť oboznámené s postupmi označovania. Všetci zamestnanci by mali absolvovať potrebné školenie, aby sa zabezpečilo správne označovanie informácií a náležité zaobchádzanie s nimi.

Aktívum vs informačné aktívum

- **Aktívum** - programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaná osoba, dobré meno orgánu riadenia a informácia, dokumentácia, zmluva a iná skutočnosť, ktorú považuje orgán riadenia za citlivú. *(Zákon o ITVS §3 písm. u))*
- Klasifikačné stupne opisujú citlivosť **informácií**, **údajov** alebo ďalších s nimi spojených informačných aktív (ďalej len „**informačné aktíva**“). *(Vyhláška NBÚ č.227/2025 Z.z., Príloha č.2)*

Aktíva podľa Vyhlášky č. 179/2020 Z.z.

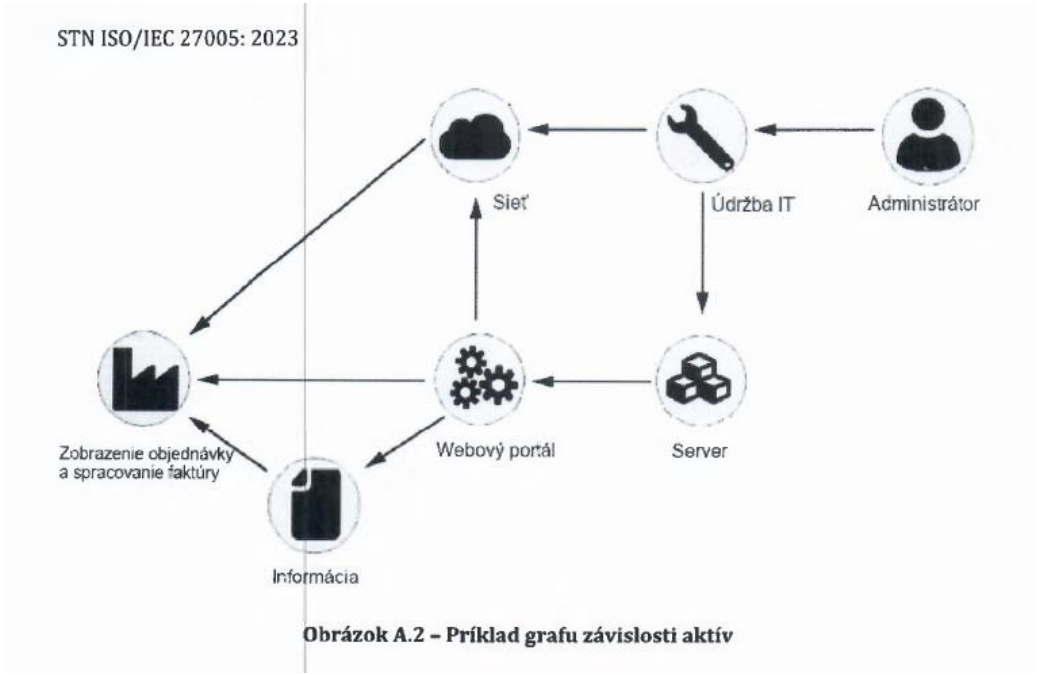
- Zoznam aktív obsahuje označenie operačného systému alebo firemného softvéru a jeho aktuálne používanej verzie všetkých týchto komponentov informačných technológií verejnej správy (Príloha 1):
  a) pracovná stanica – stolová,
  b) pracovná stanica – prenosná,
  c) aplikačný softvér,
  d) kancelársky softvér,
  e) internetový prehliadač,
  f) antivírusový softvér,
  g) komunikačný softvér,
  h) ďalší využívaný komerčný softvér,
  i) všetky druhy serverov,
  j) virtualizačné prostredie,
  k) databázové prostredie,
  l) komerčný podnikový softvér,
  m) sieťový firewall,
  n) sieťový router,
  o) sieťový prepínač,
  p) komunikačné prostredie,
  q) zálohovacie prostredie,
  r) mobilné zariadenia,
  s) dátové úložiská,
  t) ostatné zariadenia alebo sieťové prvky schopné komunikovať so zvyškom ekosystému informačných technológií verejnej správy,
  u) prenosné zariadenia.

Aktívum vs informačné aktívum

- Aktíva možno rozdeliť do divoch kategórií (STN ISO/IEC 27005:2023):

  a) **primárne/prevádzkové aktíva - informácie** alebo **procesy**, ktoré majú pre organizáciu hodnotu;

  b) **podporné aktíva - komponenty informačného systému**, na ktorých je závislé jedno alebo viacero prevádzkových aktív.



Obrázok A.2 – Príklad grafu závislosti aktív

Aktívum vs informačné aktívum

- **Aktívum** (asset) je čokoľvek, čo má pre organizáciu hodnotu. V kontexte informačnej bezpečnosti možno rozlišovať dva druhy aktív (STN ISO/IEC 27002:2023):

  a) **Primárne (prevádzkové) aktíva**:
     i. informácie;
     ii. obchodné procesy a činnosti;

  b) **podporné aktíva** (na ktoré sa primárne aktíva spoliehajú) všetkých typov, napríklad:
     i. hardvér;
     ii. softvér;
     iii. sieť;
     iv. personál (ako riadiaci orgán, vrcholový manažment, zamestnanci, dočasní zamestnanci, dodávatelia a dobrovoľníci);
     v. lokalita;
     vi. štruktúra organizácie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Aktívum vs informačné aktívum

- Príklady podľa STN ISO/IEC 27005:2019:
  - a) **Hardvér**: zariadenia na spracovanie dát, mobilné zariadenie, pevné zariadenie, spracovateľské periférie, médiá.
  - b) **Softvér**: operačný systém, SW zabezpečujúci služby, balíkový alebo štandardný SW, podnikateľské aplikácie,
  - c) **Sieť:** napr. verejná komutovaná telefónna sieť (PSTN), ethernet, gigabitový ethernet, asymetrická digitálna účastnícka prípojka (ADSL), špecifikácia bezdrôtového protokolu (napríklad WiFi 802.11), Bluetooth, FireWire, sieťové prvky (router, rozbočovač, prepínač),
  - d) **Personál:** manažment, správa a riadenie ľudských zdrojov, finančný manažment, manažér pre riziká, administrátori systému, administrátori dát, zálohovanie, helpdesk, operátor na využitie aplikácií, bezpečnostní pracovníci, vývojári, ostatní zamestnanci.
  - e) **Lokalita:** Domácnosti zamestnancov, priestory iných organizácií, prostredie mimo lokalitu (mestská oblasť, riziková oblasť), kancelárie, rezervovaná prístupová zóna, bezpečná zóna, inžinierske siete,
  - f) **štruktúra organizácie**: audítori, organizačné zložky, subdodávatelia/dodávatelia, výrobcovia.

Aktívum vs informačné aktívum

- **Informácia** (information) predstavuje aktívum, ktoré rovnako ako ďalšie dôležité aktíva organizácie sú podstatné pre činnosť organizácie a vyžadujú zodpovedajúcu ochranu. (STN ISO/IEC 27000:2023)
- **Informácia** (Information) - zmysluplné údaje (data).
- Pozn.: V kontexte systémov správy aktív IT môžu byť informáciami údaje, ktoré boli konvertované, analyzované, interpretované alebo zostavené, ktorým je priradený význam podľa kontextu a predpokladaných konvencií. Podkladové údaje sa môžu týkať objektov, ako sú fakty, udalosti, veci, procesy alebo myšlienky vrátane pojmov, ktoré majú v určitom kontexte osobitný význam súvisiaci s aktívami IT.
- Pozn.: V súvislosti so systémami správy aktív IT sa informácie môžu zaznamenávať digitálne alebo fyzicky (napr. na papieri). (ISO/IEC 19770-1:2014)
- **Údaj** (data) - fakty o objekte. (ISO/IEC 19770-1:2014)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Atribúty informácií podľa STN ISO/IEC 27000:2023

- **Dôvernosť** (confidentiality) je vlastnosť, že informácia nie je dostupná alebo nie je sprístupnená neoprávneným jednotlivcom, entitám alebo procesom.
- **Integrita** (integrity) zabezpečenie presnosti a úplnosti.
- **Dostupnosť** (availability) je vlastnosť vyjadrujúca prístupnosť a použiteľnosť na žiadosť oprávnenej entity.
- **Autenticita** (authenticity) jevlastnosť vyjadrujúca, že entita je tým, za čo sa vyhlasuje.
- **Nepopierateľnosť** (non-repudiation) schopnosť preukázať výskyt údajnej udalosti alebo činnosti a entít, ktoré ju vyvolali.
- **Spoľahlivosť** (reliability) súlad medzi zamýšľaným správaním a výsledkami.

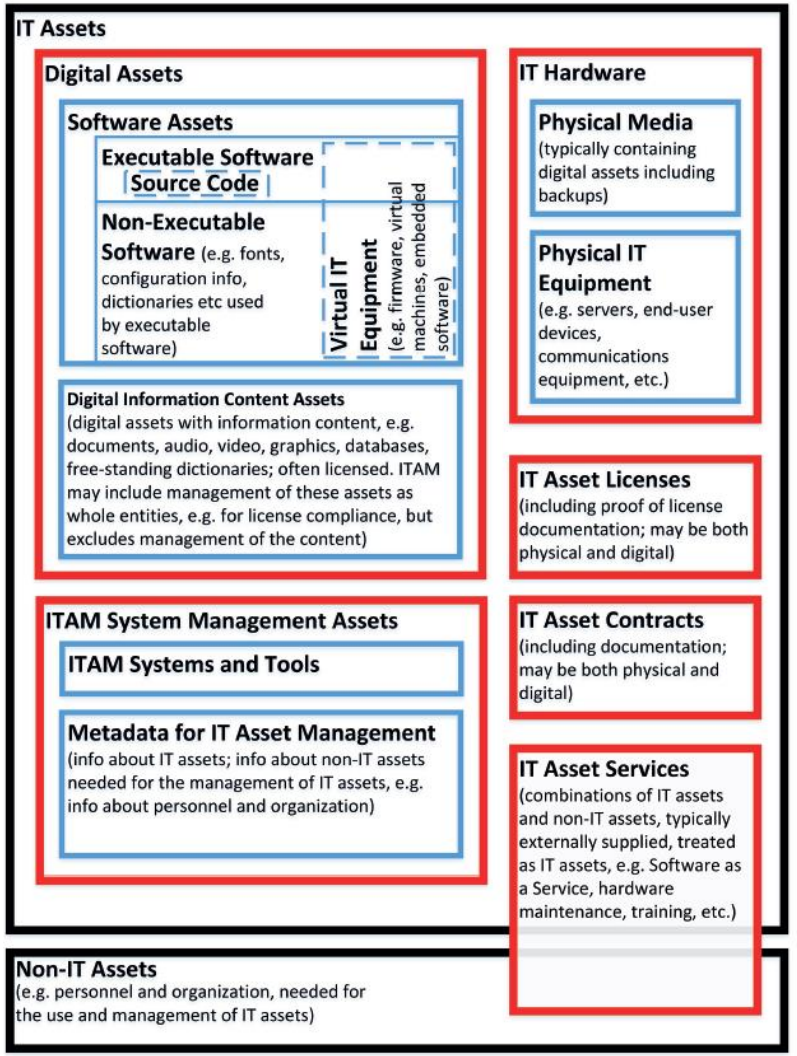
Aktívum vs. informačné aktívum

- **Informačné aktívum** (information asset) znalosti alebo údaje, ktoré majú hodnotu pre jednotlivca alebo organizáciu. (ISO/IEC 27032)
- **Fyzické aktívum** (physical asset) sú aktíva, ktoré majú hmotnú alebo materiálnu existenciu. (ISO/IEC 27032)
- **Virtuálne aktívum** (virtual asset) reprezentácia aktíva v kyberpriestore. (ISO/IEC 27032) (napr. online identita)

- **Proces** (process) je súbor aktivít majúcich vzájomný vzťah alebo vzájomne na seba pôsobiacich a premieňajúcich vstupy na výstupy. (STN ISO/IEC 27000:2023)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Aktívum vs. informačné aktívum



ISO/IEC 19770-1:2017 Správa aktív IT – Systémy správy aktív IT - Požiadavky

Informačný systém vs. sieť

- **Informačný systém** (information system) súbor aplikácií, služieb, aktív informačných technológií alebo iných komponentov na spracovanie informácií. (STN ISO/IEC 27000)
- **Informačný systémom** je funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov. (Zákon o KB).
- **Informačný systém** je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov. (Zákon o ITVS)
- **Informačným systémom verejnej správy** je informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby. (Zákon o ITVS)
- **Informačný systém** je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. (GDPR).

Informačný systém vs. sieť

- Iné definície informačného systému (Makatura, 2024):
  a) ľudia, dáta, procesy a technológie na správu informácií“ (STN EN ISO/IEC 2382-37: 2022),
  b) „infraštruktúra + aplikácie + procesy“ (ITIL4),
  c) „kombinácia prevádzkovej, dátovej, aplikačnej a technologickej architektúry“ (TOGAF9),
  d) „IT komponenty, procesy a dáta umožňujúce podnikové operácie“ (COBIT2019),
  e) „hardvér, softvér, dáta, siete a ľudia na podporu cieľov“ (NIST SP 800-53).
- **Sieť** je sieť, ktorú tvoria prenosové systémy, ktoré môžu, ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej správe kapacity, prípadne prepájacie alebo smerovacie zariadenia a iné prostriedky, vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými vlnami, optickými alebo inými elektromagnetickými prostriedkami vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním paketov vrátane internetu, mobilných sietí, elektrických vedení určených na prenos a distribúciu elektriny v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na druh prenášaných informácií. (Zákon o elektronických komunikáciách)

Informačný systém vs. sieť

- **Webové sídlo** ucelený súbor webových stránok v pôsobnosti jedného správcu, ktorý má pridelenú najmenej jednu doménu a je prezentačným komponentom a technologickým rozhraním informačného systému verejnej správy (Zákon o ITVS)
- **Technologická infraštruktúra** sústava vzájomne prepojených technických prostriedkov a programových prostriedkov umožňujúcich implementáciu a prevádzku informačných systémov verejnej správy. (Zákon o ITVS)

Manažment aktív podľa ISO 55000:2014

- **Systém manažmentu aktív** (asset management system) – systém manažmentu pre manažment aktív, ktorého funkcia je stanovenie politiky manažmentu aktív a cieľov manažmentu aktív. Požiadavky na systém sú uvedené v ISO 55001:2014.
- **Aktívum** (asset) - položka, vec alebo entita, ktorá má potenciálnu alebo skutočnú hodnotu pre organizáciu.
- **Typ aktív** je zoskupenie aktív, majúcich spoločné charakteristiky, ktoré vymedzujú tieto aktíva ako skupinu alebo triedu (napr. aktíva informačných a komunikačných technológií).
- **Kritické aktívum** (critical asset) je aktívum s potenciálom výrazne ovplyvniť dosahovanie cieľov organizácie.
- **Systém aktív** je súbor vzájomne pôsobiacich alebo vzájomne súvisiacich aktív.

Všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)

- **Operačné technológie (OT)** predstavujú hardvér a softvér používaný na monitorovanie a riadenie fyzických procesov v priemyselných a infraštruktúrnych systémoch. OT je bežne využívaná v sektoroch ako energetika, výroba, doprava, zdravotníctvo a kritická infraštruktúra.
- **Priemyselné riadiace systémy (ICS)** sú podskupinou OT a zahŕňajú rôzne typy riadiacich systémov, ako napríklad SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control System) a PLC (Programmable Logic Controller). ICS umožňujú automatizáciu, kontrolu a monitorovanie priemyselných procesov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)

- **Hlavné súčasti OT/ICS**

a) **SCADA (Supervisory Control and Data Acquisition)** – systém dohľadu a zberu dát používaný na riadenie rozľahlých priemyselných procesov.

b) **DCS (Distributed Control System)** – systém distribuovaného riadenia využívaný v rafinériách, elektrárňach a veľkých výrobných prevádzkach.

c) **PLC (Programmable Logic Controller)** – programovateľný logický automat, ktorý vykonáva riadiace funkcie v priemyselných aplikáciách.

d) **HMI (Human-Machine Interface)** – rozhranie medzi operátorom a riadiacim systémom, ktoré umožňuje vizualizáciu a ovládanie procesov.

e) **RTU (Remote Terminal Unit)** – diaľkový terminálový modul, ktorý zbiera údaje zo senzorov a posiela ich do SCADA systému.

f) **Senzory a akčné členy** – fyzické zariadenia, ktoré zabezpečujú zber dát a ovládanie procesov (napr. teplotné senzory, ventily, motory).

Všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)

Faktor	OT (Operačné technológie)	IT (Informačné technológie)
Primárny účel	Riadenie a monitorovanie fyzických procesov	Správa a spracovanie dát
Dôraz na	Dostupnosť a spoľahlivosť	Dôvernosť a integrita dát
Životný cyklus	10 – 20 rokov	3 – 5 rokov
Aktualizácie	Zriedkavé, citlivé na výpadky	Pravidelné
Protokoly	Priemyselné (Modbus, DNP3, Profibus)	Bežné sieťové protokoly (TCP/IP)

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002)

- Medzinárodná norma ISO/IEC 27002 je určená pre organizácie všetkých typov a veľkostí. Používa sa ako referencia na určenie a implementáciu opatrení na ošetrenie rizík informačnej bezpečnosti v systéme riadenia informačnej bezpečnosti (ISMS) založenom na ISO/IEC 27001.
- Organizačné alebo prostrediu špecifické opatrenia odlišné od opatrení zahrnutých v norme, je možné určiť prostredníctvom posúdenia rizík podľa potreby.
- Norma poskytuje všeobecnú kombináciu organizačných, ľudských, fyzických a technologických opatrení informačnej bezpečnosti odvodených z medzinárodne uznávaných osvedčených postupov.
- Pri špecifikovaní takýchto opatrení by organizácia mala zvážiť zdroje a investície potrebné na implementáciu a prevádzku opatrení s realizovanou obchodnou hodnotou.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002)

- Mala by existovať rovnováha medzi zdrojmi nasadenými na implementáciu opatrení a potenciálnym vplyvom bezpečnostných incidentov pri absencii týchto opatrení na podnikanie.
- Výsledky posúdenia rizík by mali pomôcť usmerňovať a určiť vhodné kroky, priority pre riadenie rizík informačnej bezpečnosti a na implementáciu opatrení nevyhnutných na ochranu pred týmito rizikami.
- Viac informácií o určovaní opatrení a iných možností ošetrenia rizík je možné nájsť v ISO/IEC 27005.
- Aj keď norma ponúka usmernenie týkajúce sa širokého spektra opatrení informačnej bezpečnosti, ktoré sa bežne uplatňujú v rôznych organizáciách, ďalšie dokumenty z radu noriem ISO/IEC 27000 poskytujú doplňujúce informácie alebo požiadavky.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002)

- Existujú normy špecifické pre odvetvie, ktoré obsahujú ďalšie opatrenia, ktorých cieľom je riešiť konkrétne oblasti (napr. ISO/IEC 27017 pre cloudové služby, ISO/IEC 27701 pre ochranu osobných údajov, ISO/IEC 27019 pre energetický priemysel, ISO/IEC 27011 pre telekomunikačné služby a ISO 277999 pre oblasť zdravotníctva).
- Norma je štruktúrovaná do nasledujúcich kapitol/tém:
  a) Organizačné opatrenia (kapitola 5).
  b) Personálne opatrenia (kapitola 6).
  c) Fyzické opatrenia (kapitola 7).
  d) Technické opatrenia (kapitola 8).
- Príloha A - Používanie atribútov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Témy a atribúty

- Organizácia môže používať atribúty na vytváranie rôznych náhľadov, ktoré predstavujú odlišné kategorizácie opatrení z iného uhla pohľadu na rozdiel od tém. Atribúty možno použiť na filtrovanie, triedenie alebo prezentáciu opatrení v rôznych zobrazeniach pre rôzne publikum. V prílohe A sa vysvetľuje, ako to možno dosiahnuť, a uvádza sa príklad zobrazenia.

Témy a atribúty

- Ku každému opatreniu bolo priradených päť atribútov s príslušnými hodnotami atribútov (pred ktorými je znak „#“, aby sa dali vyhľadávať), a to:

a) **Typ opatrenia:** Typ opatrenia je atribút, ktorý slúži na zobrazenie opatrení z hľadiska toho, kedy a ako opatrenie modifikuje riziko vzhľadom na výskyt incidentu informačnej bezpečnosti. Možné hodnoty atribútu sa skladajú z :
   - **Preventívne** (opatrenie, ktorá má zabrániť vzniku incidentu informačnej bezpečnosti),
   - **Detekčné** (opatrenie pôsobí pri vzniku incidentu informačnej bezpečnosti),
   - **Nápravné** (opatrenie pôsobí po vzniku incidentu informačnej bezpečnosti).

Témy a atribúty

b) **Vlastnosti informačnej bezpečnosti:** Vlastnosť informačnej bezpečnosti je atribút, ktorý umožňuje nahliadať na opatrenia z hľadiska toho, k zachovaniu ktorých vlastností informácií opatrenie prispeje. Možné hodnoty atribútu pozostávajú z **Dôvernosť**, **Integrita** a **Dostupnosť**.

c) **Koncepty kybernetickej bezpečnosti:** Koncept kybernetickej bezpečnosti je atribút na zobrazenie opatrení z hľadiska prepojenia opatrení s konceptmi kybernetickej bezpečnosti definovanými v rámci kybernetickej bezpečnosti popísanom v norme ISO/IEC TS 27110 Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia - Smernice pre vývoj rámca kybernetickej bezpečnosti. Možné hodnoty atribútu pozostávajú z **Identifikovať**, **Chrániť**, **Objaviť**, **Reagovať**, **Obnoviť**.

Témy a atribúty

d) **Prevádzkové možnosti**: Prevádzkové možnosti sú atribútom, ktorý umožňuje nahliadať na opatrenia z pohľadu odborníka na informačnú bezpečnosť. Možné hodnoty atribútu pozostávajú z nasledovných oblastí: **Riadenie**, **Správa aktív**, **Ochrana informácií**, **Bezpečnosť ľudských zdrojov**, **Fyzická bezpečnosť**, **Systémová a sieťová bezpečnosť**, **Aplikačná bezpečnosť**, **Bezpečná konfigurácia**, **Správa identít a prístupov**, **Správa hrozieb a zraniteľností**, **Kontinuita**, **Bezpečnosť dodávateľských vzťahov**, **Právo a súlad**, **Riadenie udalostí informačnej bezpečnosti** a **Uistenie o informačnej bezpečnosti**.

Témy a atribúty

e) **Bezpečnostné domény:** Bezpečnostné domény sú atribútom na zobrazenie opatrení z pohľadu štyroch domén informačnej bezpečnosti:

1) „**Riadenie a ekosystém**“ zahŕňa „Riadenie bezpečnosti informačných systémov a riadenie rizík“ a „Riadenie kybernetickej bezpečnosti ekosystému“ (vrátane interných a externých zainteresovaných strán);
2) „**Ochrana**“ zahŕňa „Bezpečnostnú architektúru IT“, „Správu bezpečnosti IT“, „Riadenie identít a prístupu“, „Údržbu bezpečnosti IT“ a „Fyzickú bezpečnosť a bezpečnosť prostredia“:
3) „**Obrana**" zahŕňa „Detekciu“ a „Riadenie incidentov počítačovej bezpečnosti“;
4) „**Odolnosť**“ zahŕňa „Kontinuitu prevádzky“ a „Krízové riadenie“.

Témy a atribúty

5 Organizačné opatrenia

5.1 Politiky informačnej bezpečnosti

Typ opatrenia	Vlastnosti informačnej bezpečnosti	Koncepty kybernetickej bezpečnosti	Prevádzkové možnosti	Bezpečnostné domény
#Preventívne	#Dôvernosť #Integrita #Dostupnosť	#Identifikovať	#Riadenie	#Riadenie_a_ekosystém #Odolnosť

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Štruktúra opatrení

- Rozloženie každého opatrenia obsahuje nasledujúce položky:
    a) Názov opatrenia: Krátky názov opatrenia;
    b) Tabuľka atribútov: Tabuľka zobrazuje hod-noty jednotlivých atribútov pre dané opatrenie;
    c) Opatrenie: Čo je opatrenie;
    d) Účel: Prečo by sa malo opatrenie zaviesť;
    e) Návod: Ako by sa malo opatrenie implementovať';
    f) Ďalšie informácie: Vysvetľujúci text alebo odkazy na iné súvisiace dokumenty.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Správa aktív, ochrana záznamov, súkromia a označovania informácií

Právny rámec, organizácia KB a strategické plánovanie (Blok I)

Kurz: Manažér kybernetickej bezpečnosti

prof. Ing. Tomáš Loveček, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Tomas.Lovecek@uniza.sk